Please type a plus sign (+) inside this box → +

Docket Number: SSO-10018/29

PROVISIONAL APPLICATION FOR PATENT COVER SHEET (Small Entity)

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53 (c).

INVENTOR(S)/APPLICANT(S)		
Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
Ryan Mark	Sherman Sendo	Royal Oak, Michigan Ann Arbor, Michigan

☐ *Additional inventors are being named on page 2 attached hereto*

TITLE OF THE INVENTION (280 characters max)

ELECTRONIC MONEY APPARATUS AND METHODS

CORRESPONDENCE ADDRESS

Direct all correspondence to:

☐ Customer Number [ ] → *Place Customer Number Bar Code Label here*

OR

☒ Firm or Individual Name	John G. Posa				
Address	Gifford, Krass, Groh et al				
Address	280 N. Old Woodward Ave., Suite 400				
City	Birmingham	State	MI	ZIP	48009
Country	US	Telephone	734/913-9300	Fax	734/913-6007

ENCLOSED APPLICATION PARTS *(check all that apply)*

☒ Specification	*Number of Pages*	6	☒ Small Entity Statement		
☒ Drawing(s)	*Number of Sheets*	3	☐ Other (specify)		

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT *(check one)*

		FILING FEE AMOUNT
☒	A check or money order is enclosed to cover the filing fees	
☐	The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number: [ ]	$75.00

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____

Respectfully submitted,

SIGNATURE _____ Date 04/28/1999

TYPED or PRINTED NAME John G. Posa REGISTRATION NO. *(if appropriate)* 37,424

TELEPHONE 734/913-9300

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

SEND TO: Box Provisional Application, Assistant Commissioner for Patents, Washington, DC 20231

P19SMALLREV04

PROVISIONAL APPLICATION FOR PATENT COVER SHEET (Small Entity)

INVENTOR(S)/APPLICANT(S)		
Given Name (first and middle [if any])	Family Name or Surname	Residence (city and either State or Foreign Country)

Certificate of Mailing by Express Mail

I certify that this provisional patent application cover sheet, provisional patent application and fee is being deposited on **April 28, 1999** with the U.S. Postal Service as "Express Mail Post Office to Addressee" service under 37 C.F.R. 1.10 and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Sheryl L. Hammer

Signature of Person Mailing Correspondence

Sheryl L. Hammer

Typed or Printed Name of Person Mailing Correspondence

EJ335014771US

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

SEND TO: Box Provisional Application, Assistant Commissioner for Patents, Washington, DC 20231

Applicants: Ryan Sherman and Mark Sendo

Serial No.:

Filed:

For: ELECTRONIC MONEY APPARATUS AND METHODS

VERIFIED STATEMENT (DECLARATION) CLAIMING SMALL ENTITY STATUS (37 CFR 1.9(f) and 1.27(b)) - INDEPENDENT INVENTOR

As the below named inventor, I hereby declare that I qualify as an independent inventor as defined in 37 CFR 1.9(c) for purposes of paying reduced fees under Section 41(a) and (b) of Title 35, United States Code, to the Patent and Trademark Office with regard to the invention entitled ELECTRONIC MONEY APPARATUS AND METHODS described in

- ■ the specification filed herewith.
- ☐ application serial no. _____, filed _____.
- ☐ patent no. _____, issued _____.

I have not assigned, granted, conveyed or licensed and am under no obligation under contract or law to assign, grant, convey or license, any rights in the invention to any person who could not be classified as an independent inventor under 37 CFR 1.9(c) if that person had made the invention, or to any concern which would not qualify as a small business concern under 37 CFR 1.9(d) or a non-profit organization under 37 CFR 1.9(e).

Each person, concern or organization to which I have assigned, granted, conveyed, or licensed or am under an obligation under contract or law to assign, grant, convey, or license any rights in the invention is listed below:

- ■ no such persons, concern, or organization
- ☐ persons, concerns or organizations listed below*

**NOTE: Separate verified statements are required from each named person, concern or organization having rights to the invention averring to their status as small entities. (37 CFR 1.27)*

FULL NAME _____
ADDRESS _____
_____
☐ Individual ☐ Small Business Concern ☐ Non-Profit Organization

FULL NAME _____
ADDRESS _____
_____
☐ Individual ☐ Small Business Concern ☐ Non-Profit Organization

FULL NAME _____
ADDRESS _____
_____
☐ Individual ☐ Small Business Concern ☐ Non-Profit Organization

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28(b)).

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

Ryan Sherman
Name of Inventor

Signature of Inventor

Date 4-27-99

Mark Sendo
Name of Inventor

Signature of Inventor

Date 4/27/99

Electronic Money Apparatus and Methods

Inventors: Ryan Sherman and Mark Sendo

Overview:

Many of today's web sites claim to offer a secure method in which to transmit sensitive financial data (i.e.: to provide a credit card number for on-line purchases). Despite these claims, electronic transactions are always susceptible to theft. It has been extensively published that the lack of a totally secure method for monetary transactions across the net continues to plague cyberspace transactions and remains the number one problem with Internet commerce. There has been substantial time and effort devoted to the SET (secure electronic transaction) standard, which is designed to be an industry-wide protocol for transmitting sensitive personal and financial information over public networks. Many sophisticated encryption techniques, such as SSL (Secure Socket Layer), TLS, IPSec, S/MIME, and others have been used in an effort to elude cyber-thieves (hackers) from obtaining this data. The problem is that for every new method implemented, there will always be a hacker who can break the code. This has been a fact of life from the beginning of time. Dating back to the first banks, bank robbers have been able get into safes and steal the goods using a variety of techniques. They can pick the lock, blow up the lock, force a bank employee to open the safe, or use inside information (a conspirator with bank knowledge) to gain access. Throughout the centuries and into cyberspace, nothing has changed. As encryption and copy protection have become more advanced, so have the methods of hackers. The only reason that the original encryption protocol is no longer in use is because a hacker has broken it. This is also true of the second method, the third, and so on. It is only a matter of time before today's encryption methods are obsolete, and this race to out-smart the hackers is futile. With any supposed "secure" transaction on the Internet today, the buyer assumes the risk of credit card number theft because a hacker can break the encryption protocol at any time. In a sense, there can never be a totally safe method for transmitting a credit card number over the Internet.

The fact that credit card transactions can never be safe does not mean that the integrity of Internet purchases need always be compromised. All that is required is a method for conducting electronic monetary transactions which does not require the electronic data to be secure. Since security always runs the risk of being compromised, a system needs to be developed whereby the data being transmitted is not of a sensitive nature, and the theft of this data is of no detrimental consequence to the transmitter or receiver of the data. The real world analogy would be a customer handing over cash to a clerk in a department store. If people who are standing around happen to see the transaction, or even read the serial numbers on the currency, it is of no detrimental consequence to any party. In cyberspace, this presents somewhat of an obstacle since we cannot transmit cash over a phone line.

Up until this point, there existed no known solution to the problem of securing on-line monetary transactions. The inventors have found such a solution. The criteria for such a solution are:

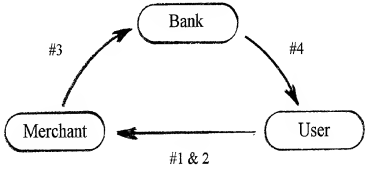
the numerical data being transmitted by the buyer during the purchase must not be sensitive in nature, yet must represent a valid coded combination which is equivalent to a specific monetary value;

once the numerical data is transmitted, subsequence use of that data must no longer represents any monetary value;

upon receipt of the transmitted data, the merchant must be able to instantly verify that the data is a legitimate representation of a specific value for which he/she will be paid;

numerical data representing monetary value which is being downloaded from source of issuance (bank) to the user must not be sensitive in nature, yet must contain data which is capable of producing a valid numerical code via manipulation.

The above four criteria represent the data transmissions in the following diagram:



The above four criteria are fully met by a revolutionary transactional process created by the inventors. Although a final name for this new process has not been determined, an interim name of "ecash" will be used to reference this protocol of information transfer and numerical coding. Ecash, the process, is the first of two ideas that the inventors wish to patent.

ECASH: Bullet-proof security:

Using ecash, there is literally no concern over the security or theft of electronic transactions because as the coded numbers representing the currency are transmitted for use, they are expunged from the system and unavailable for future use. It is the equivalent of handing over a dollar bill to the cashier at a store, not worrying if the next person in line sees the serial number on your dollar bill. As soon as the bill is handed to the cashier, it cannot be used again at that store. Even better than this analogy, as soon as ecash is spent, it cannot ever be spent again. Each cyber-dollar issued is assigned a unique 16-digit alphanumeric number. Once that dollar, with its associated unique tracking number, is spent (by being transmitted across the web to the merchant), that number is removed from circulation. This prevents any possibility of theft and reuse via duplication. Furthermore, because of the vast

number of 16-digit alphanumeric combinations, each cyber-dollar contains an intrinsic code making the odds of randomly "guessing" a valid number mathematically impossible. The flow of information during a transaction makes it impossible for a "hacker" to make multiple high-speed guesses of valid tracking numbers. Every number is submitted to the host system via the merchant. A single invalid number is flagged and that merchant is not permitted to submit a subsequent transaction until the cause of the invalid number is determined.

A key to this system is the fact that each cyber-dollar has a unique 16-digit alphanumeric tracking number. The number of possible combinations using this many digits is approximately 7.95 septillion (or a 7 followed by 24 zeroes). With this large number, currency will never need to be reused. If the entire earth's population (approximately 4 billion people), each were issued $1 billion per year, it would take approximately 8 million years to use all of the currency. This allows several extra digits in each tracking number to mathematically relate to one another, which could be used as an additional method of differentiating valid from invalid tracking numbers. This is not required since each number will be entered into the host database upon issuance. Furthermore, even if a "hacker" was allowed multiple attempts at trying to "guess" a valid number via a high-speed computer, it would take 8 trillion years to guess a valid number at a rate of one million submitted guesses per second.

In order to accomplish the above-described electronic transactions, the user of the ecash system must possess a means of storing and dispensing the numerical data representing the monetary value. This could be accomplished with an existing storage device such as a 3.5 inch diskette. However, the inventors have created a new, revolutionary device to accomplish this task. This new device is temporarily being called the Internet Money Card ("iMC"), and is the second invention to be patented.

iMC – The cyber-card of the next century:

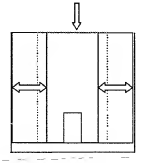
The Internet money card (iMC) is a unique, specialized data storage device which will contain the coded data which is used in the ecash transactions. It is the intention of this patent to protect all possible designs for such a device. A first generation design would be a diskette that transforms from a standard sized 3.5 inch diskette to the size of a standard credit card. This card will contain the numerical data strings that represent monetary value for on-line Internet purchases. In expanded mode, it will easily slide into any 3.5 inch diskette drive which can be found on virtually every personal computer manufactured today. In collapsed mode, it will slide into any wallet or purse with the same ease as a typical credit card.

Upon issuance to the user, the card contains a hidden, encrypted code which will integrate with downloaded numeric data strings to form valid data codes representing monetary value. This pre-coded information makes it impossible for any standard 3.5 diskette, or any other magnetic media device, to be used for ecash transactions.

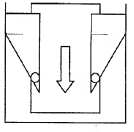
The outer diameter of the inner magnetic flimsy disk is limited by the dimensions of the protective case, which collapses to the width of a credit card. Because this diameter is significantly less than that of a standard 3.5 inch diskette, data storage capacity is reduced, and the distance the circular storage disk extends into the drive is reduced. When the drive is first recognized by the computer system, the read/write head searches for the file allocation table (FAT) which is located at the interior portion of the disk. The FAT of the iMC will only instruct the read/write head of the drive to search areas where data are stored. This will eliminate drive errors due to the lack of magnetic media under the entire length of head track.

There are several designs which will accomplish the goal of a 3.5 inch diskette collapsing to the size of a credit card. It is the process of collapsing and expanding between the two sizes which is a novel idea. A patent should protect the gamut of configurations which accomplish this goal.

One method of transformation consists of a credit card sized diskette with two metal protective sleeves covering the length of each side. On a standard 3.5 inch diskette, there is one (short) protective metal sleeve covering the sensitive data disk along the front edge of the diskette. These two sleeves will extend out to each side bringing the overall width to 3.5 inches. They can snap into place using a simple spring and groove system, with track and grooving used similar to the protective sleeve on traditional 3.5 inch diskettes. Alternatively, the two sleeves can slide across a J-shaped groove track to lock into place. To collapse the diskette back to its credit card size, simply pull the sleeve outward a fraction of an inch, then forward, and it will snap back to its reduced size if using the J-grooves with a spring mechanism. The final engineering design is yet to be determined. A top view of a possible configuration appears as follows:



Another method of transformation consists of a credit card sized diskette with a hinged wing on each side. These wings are affixed with a standard rivet-style pin protruding through the diskette. When extended, a top view of the diskette will resemble a stealth fighter plane, where the wing tips will be 3.5 inches apart to stabilize the lateral movement of the iMC in the drive. Such a design appears as follows:



Since the width of the iMC is only 2 1/8 inches, as compared to the 3 ½ inches of a standard diskette, the surface area of the circular magnetic storage area contained within the iMC will be significantly less than that of a standard diskette. Using surface area computations, a standard diskette contains approximately 2.4 square inches of usable data storage space. The iMC circular magnetic disk contains approximately .2 square inches of usable data storage space. Using today's standard formatting patterns, the 2.4 square inches of a standard diskette holds 1.44 Mb (megabytes) of data (i.e.: 1,475,560 bytes of data). Each byte contains 8 bits, where each bit is a binary digit. With the reduced circular diameter and surface area of the iMC, the data capacity is 120,000 bytes. If a slightly enlarged card width is used, such as 2 5/8 inches, the data capacity increases to 471,000 bytes.

As computer technology evolves, so will the iMC. The initial design is a collapsible diskette designed to fit in a 3.5 inch standard diskette drive. The reason for this initial method of data interchange is because virtually all computer systems on the market today, both desktop and laptop units, contain a 3.5 inch drive. Other technologies will gradually become more accepted and the iMC will adapt and change with the industry. Just as music evolved through 8 track tapes, cassette tapes, and CD's, the iMC will evolve through a 3.5 inch diskette, a true credit card with a magnetic strip, and into designs that will be compatible with hardware that hasn't been released yet. As plug and play technology evolves, the iMC may interface with other sources of data entry into a computer. In addition to the 3.5 inch diskette drive, the iMC may be designed to interface with a serial or parallel port (COM or LPT), a modem card (or RJ11 jack), a PCMCIA socket, a network port, or any other port that can be used for data exchange.

As the field of biometrics advances, the iMC will incorporate these techniques for advanced encryption and verification of authenticity. When a user inserts their iMC (or swipes it through their card reader), the accompanying software may require verification from the user's finger print, voice, retinal scan, and other unique human characteristics.

The inventors realize that technologies (such as credit cards with magnetic strips) currently exist for data transfer. It is the use of these technologies specifically for the encryption, storage, and usage of data for the process of ecash Internet currency exchange that the inventors wish to protect. The initial method of using a collapsible 3.5 inch diskette should be fully protected since it does not currently exist.

Coding:

The data representing monetary value are coded onto the iMC using a unique encryption technique, which for security purposes, can only be presented in general terms. The base unit of currency is one U.S. dollar. There are no subdivisions of the base unit, and all purchases made must be rounded to the nearest dollar. All users of the ecash system and all merchants accepting ecash as payment will contractually agree to this stipulation during

registration. Each dollar is represented on the iMC as a coded 16 digit alphanumeric number (called an AN string). Although one byte of data is capable of 256 permutations, each digit of the AN string will be assigned one byte, for a total memory storage space of 16 bytes per AN string. Special encryption may or may not utilize the balance of unused memory (since each digit of an AN string requires 36, not 256, permutations). With each AN string (or ecash dollar) utilizing 16 bytes of iMC storage space, the 120,000 byte usable surface will store approximately 7500 AN strings, or the equivalent of $7500.00 per iMC card. The slightly enlarged version of the iMC could hold approximately 29,437 AN strings, or $29,437.

Security during withdrawals (downloads):

The user applies more monetary value to his iMC by making a withdrawal from the inventors' electronic bank on-line. The natural security issue raised here is whether the AN strings can be intercepted while being transferred from the bank to user, allowing the hacker to spend the funds before the entitled user makes purchases. This illegal interception is prevented in two ways: First, each iMC is initially delivered with a two-digit code encrypted and hidden on the disk. The AN strings downloaded to the user are 12 digits each initially. The two digit code from the iMC is added to each iMC to make the AN string 14 digits. Secondly, with each withdrawal (download), a hundred extra random AN strings are sent which are used to mask another two-digit code. This code is added to the (now) 14 digit AN string to complete the final 16 digit sequence. This full 16-digit sequence is what is recorded in inventors' host computer. If a hacker intercepts a withdrawal (a download), then he/she will only intercept a 12-digit number which will not be valid. In addition, if they happen to know the user's 2-digit code hidden on the disk, the 16 digit AN string is still not complete. Finally, if the hacker can miraculously decipher the two digits masked in the extraneous data dump, then the hacker would still need to know the two digits hidden on the iMC itself. Since this information is not available even to the legitimate iMC user, the chance that a hacker can obtain this information is not realistic.

Summary:

The inventors wish to file two patents, with each patent listing both inventors with equal status. The first patent should protect the process of transacting Internet monetary transactions via a system which utilizes disposable alphanumeric data strings which correlate to monetary value. The merchant verifies the validity of the user's data by uploading the data to the inventors' host computer system, which will download the approval of the transaction and expunge the used data strings to prevent duplicate use. The second patent should protect the concept of an expandable/collapsible (from 3.5 inch diskette size to credit card size) magnetic media storage device. The primary purpose for this device is to transact secure Internet purchases as described by invention #1. The patent should further protect the general method of encoding and transmitting data as described in this document.